ORIGINAL RESEARCH

Research Review of Nongovernmental Organizations' Security Policies for Humanitarian Programs in War, Conflict, and Postconflict Environments

Elizabeth Rowley, MIA, MHS, Lauren Burns, MA, and Gilbert Burnham, MD, PhD

ABSTRACT

Objectives: To identify the most and least commonly cited security management messages that nongovernmental organizations (NGOs) are communicating to their field staff, to determine the types of documentation that NGOs most often use to communicate key security messages, and to distinguish the points of commonality and divergence across organizations in the content of key security messages.

Methods: The authors undertook a systematic review of available security policies, manuals, and training materials from 20 international humanitarian NGOs using the InterAction Minimum Operating Security Standards as the basis for a review framework.

Results: The most commonly cited standards include analytical security issues such as threat and risk assessment processes and guidance on acceptance, protection, and deterrence approaches. Among the least commonly cited standards were considering security threats to national staff during staffing decision processes, incorporating security awareness into job descriptions, and ensuring that national staff security issues are addressed in trainings. NGO staff receive security-related messages through multiple document types, but only 12 of the 20 organizations have a distinct security policy document. Points of convergence across organizations in the content of commonly cited standards were found in many areas, but differences in security risk and threat assessment guidance may undermine communication between aid workers about changes in local security environments.

Conclusions: Although the humanitarian community has experienced significant progress in the development of practical staff security guidance during the past 10 years, gaps remain that can hinder efforts to garner needed resources, clarify security responsibilities, and ensure that the distinct needs of national staff are recognized and addressed. (*Disaster Med Public Health Preparedness*. 2013;7:241-250)

Key Words: humanitarian, international, security, staff, policies

Aid workers are often called upon to work in countries before, during, or after a conflict. Even in countries considered stable, aid workers face threats such as kidnapping, detention, landmines, road ambushes, and attacks causing serious injury or death. Security-related violence is a leading cause of death and serious injury among aid workers.[1,2] Two studies estimate intentional violence events at 6/10 000 person-years during approximately the same period ending in 2005, albeit using different nongeneralizable methods and case definitions.[2,3] Although the number of events has clearly risen between 2006 and 2008, it is unclear whether the risk of such events has increased over time outside certain high-risk countries.[4,5]

Nongovernmental organization (NGO) managers face the challenge of meeting a humanitarian mandate while ensuring the protection of their staff. Less than 10 years ago many humanitarian organizations did not have dedicated security staff or written security documents.[5-8] The evolved field of humanitarian security management now includes more staff and more complete security policies, security manuals, and security training materials, although gaps exist. A 2004 review by the European Commission Humanitarian Office asserted that the security policies and procedures of many NGOs were inadequate, noting that "security procedures are not routinely developed in consultation with all groups of staff, and do not always respond to identified threats in the context."[7] Bollettino noted that current security management practice is limited by "over reliance on static structural information found in the occasional field security assessment, and often outdated security plans and guidelines," that do not help managers look at ongoing changes in security,[4] and Stoddard, Harmer,

TABLE 1

InterAction Minimum Operating Security Standards, 2006*

Standard No.	Standard Topic	Description of Standard
1	Organizational security policy and plans	InterAction members shall have policies addressing key security issues and formal plans at both field and headquarters levels to address these issues.
2	Resources to address security	InterAction members shall make available appropriate resources to meet these minimum operating security standards.
3	Human resources management	InterAction members shall implement reasonable hiring polices and personnel procedures to prepare staff to cope with the security issues at their posts of assignment, support them during their service, and address postassignment issues.
4	Accountability	InterAction members shall incorporate accountability for security into their management systems at both field and headquarters levels.
5	Sense of community	InterAction members shall work in a collaborative manner with other members of the humanitarian and development communities to advance their common security interests.

*http://www.eisf.eu/resources/library/IA_MOSS_1.pdf.

and DiDomenico observed that policies and programmatic frameworks, designed to help aid workers function in highly volatile environments such as Darfur, Afghanistan, and Somalia, "appear inadequate to protect staff and operations."[5]

In early 2009, the Bureau of International Cooperation of the International Medical Center of Japan asked the Center for Refugee and Disaster Response of the Johns Hopkins Bloomberg School of Public Health to document security measures that are common to international NGOs. This documentation entailed the review of available security policies, manuals, and training materials from 20 international NGOs with 3 main objectives:

1. Identify the most and least commonly cited security management messages that NGOs are communicating to their field staff.
2. Determine the types of documentation NGOs most often use to communicate key security messages.
3. Distinguish the points of commonality and divergence across organizations in the content of key security messages.

InterAction, a coalition of US-based international NGOs, developed the InterAction Minimum Operating Security Standards (MOSS) in 2006[9] (Table 1) as a foundation for institutional security strategies. NGOs belonging to InterAction are required to certify that they are MOSS compliant or taking specific steps to achieve MOSS standards. Although subject to interpretation across organizations, suggested implementing guidance for the InterAction MOSS lists specific components that should be considered within each standard.[10] The InterAction MOSS was chosen as a framework for the systematic review of materials based on its comprehensiveness.

METHODS

Research staff contacted the humanitarian NGO community about the review primarily through InterAction (through the senior security coordinator) and the European Interagency Security Forum (through the coordinator). Key staff at each of these coordination organizations e-mailed member NGOs, describing the review and inviting organizations to share their security manuals, policies and guidelines, and training materials. In addition, research staff contacted 3 Japanese NGOs and followed up with organizations that participated in earlier research.

To review the materials systematically, research staff developed a matrix of 85 security-related subcomponents, of which 73 directly apply to the suggested guidance for implementing InterAction's 5 MOSS standards and their guidelines, "The Security of National Staff: Essential Steps 2002."[11] Research staff added 12 subcomponents that were included in the materials of the 2 organizations first reviewed (Table 2). For each NGO, research staff noted all of the 85 subcomponents that were mentioned within each category of security materials (policy document, manual, training materials).

Research staff compiled the individual NGO matrices into an all-inclusive matrix to count and categorize subcomponents as most commonly, commonly, or least commonly mentioned. The highest number of times any subcomponent was mentioned was 30 times. Subcomponents mentioned 1 to 10 times were classified as least common, subcomponents mentioned 11 to 20 times were classified as common, and subcomponents mentioned 21 to 30 times were classified as most common. To distill more specific observations, research staff further categorized subcomponents based on the number of organizations, including it in any of their materials. Subcomponents mentioned by 5 or fewer organizations (ie, only 25% of the organizations) and in only 1 to 10 documents were categorized as least common. Subcomponents mentioned by 16 or more organizations (ie, 75% of the organizations) and included in 21 to 30 documents were categorized as most common. This categorization yielded a more succinct list of most and least commonly cited security-related issues (Tables 3 and 4; Results). From this list, research staff reviewed points of commonality

TABLE 2

Subcomponents Added to the MOSS for This Review

Standard No.	Description of Added Subcomponents
1	Established rules of engagement for situations in which armed security is used
1	Distinction between security and safety
1	Identification of "security phases" (or "security levels") and the origin of security categories, if applicable
1	Individual/personal security behaviors
1	Travel logistics (eg, safety and security when using hotels, public transportation, airports)
1	Organization document security (safeguarding security of sensitive information)
1	Specific guidance on prevention of and response to sexual violence
1	Specific guidance to increase land mine awareness where relevant
3	Cultural sensitivity as related to security
3	Clarity in security policies that affect national staff
4	Articulation of the individual's responsibility for carrying out his or her work in a way that supports the organization's security efforts
5	Awareness of and capacity to implement organization's stance on neutrality in both substance and appearance in specific contexts

and divergence within some of the most commonly cited subcomponents.

RESULTS

Twelve American NGOs, 7 European NGOs, and 1 Japanese NGO provided 20 security manuals, 12 policy/guideline documents, and 5 sets of training materials. Although all of the NGOs in this group have some form of security manual, formal security policy, whether embedded within guidance or presented as a stand-alone document, does not exist in all of the organizations. Many NGOs outsource some or all of their security training and therefore do not have their own training materials. Because the 5 sets of training materials that the research staff could access may not be representative of the humanitarian NGO sector in general, the review's key observations were generated mainly from security manuals and policy documents.

Coverage of the 5 Standards

Overall, most organizations devote the majority of their security document content to covering issues that are included within standard 1 (organizational security policy and plans). Only 2 of the 16 most commonly cited subcomponents are not from standard 1.

There are rarely references to concepts related to standard 2 (resources to address security). Adequate resource allocation is occasionally mentioned in relation to other specific security issues, such as the cost of certain protection measures (eg, procurement of flak jackets, specially outfitted vehicles, office security), but only 2 organizations specifically mention the need to plan systematically for the financial implications of security management. Most organizations' security policy and guidance do not fully incorporate standard 3 (human resource management), and none of the standards that are categorized as most common are from standard 3. In contrast, all but 1 of the least commonly cited security-related issues are found in standard 3. Several subcomponents under standard 3 relate to national staff through reference to InterAction's "The Security of National Staff: Essential Steps 2002," and are not commonly cited.

Standard 4 (accountability) is limited in scope as compared with other standards. Of the 4 original subcomponents under standard 4, 2 are included among those that are least commonly cited (staff evaluations to include security-related responsibilities, if any, and clearly stated consequences for violation of security policies and procedures). The added subcomponent under standard 4 (articulation of the individual's responsibility for carrying out their work in a way that supports the organization's security efforts) is among the most commonly cited.

Standard 5 (sense of community) is also limited in the number of subcomponents, with only 4 that were already part of the MOSS-implementing guidance and 1 that was added by research staff. The subcomponent related to information sharing with other humanitarian actors is 1 of the most commonly cited. In contrast, awareness of and taking steps to mitigate any negative impact of an organization's operations on the security of others is a more conceptually oriented issue that is included in the list of least frequently cited subcomponents.

Most and Least Frequently Cited Security-related Issues

Tables 3 and 4 summarize the subcomponents of the InterAction MOSS that are most and least commonly included in organizations' documents. The categorization was based on the review of all of the available documents, including training materials; however, the total scores include only security manuals and policy documents because few training materials were available. Tables 3 and 4 present subcomponents as being either conceptual/analysis-oriented or practical, a distinction that recognizes some subcomponents focus on procedural activities such as incident reporting

TABLE 3

Most Commonly Cited Issues in Organizations' Security Manuals, Policies/Guidelines, and Training Materials*

Standard No.	Description of Subcomponent	No. Organizations Citing Item in Security Manuals (of 20)	No. Organizations Citing Item in Security Policies/ Guidelines (of 12)	Total I1rhl
	Conceptual/analysis-oriented security management subcomponents			
1	Incorporation of threat/risk assessment processes in country-specific security plans	18 (90%)	8 (66%)	26
4	Articulation of individual's responsibility for carrying out his or her work in a way that supports the organization's security efforts†	16 (80%)	10 (83%)	26
1	Guidance on incorporation of acceptance, protection, and/or deterrence strategies	16 (80%)	7 (58%)	23
1	Framework for determining acceptable and unacceptable risks to staff, assets, and image of organization	14 (70%)	5 (42%)	19
1	Summary of the situation (eg, political, economic, historical, military) in local security plans	17 (89%)	1 (8%)	18
	Practical security management subcomponents			
1	Use of armed security	17 (85%)	9 (75%)	26
1	Security incident reporting requirements	18 (90%)	7 (58%)	25
1	Movement and transport (eg, vehicles, convoys) in local security plans	18 (90%)	4 (33%)	22
1	Telecommunications (regular use and during emergencies) in local security plans	18 (90%)	3 (25%)	21
1	Contingency plans for security evacuation	17 (85%)	4 (33%)	21
1	Contingency plans for medical evacuation	15 (75%)	6 (50%)	21
5	Sharing of security-related information with other humanitarian actors, as deemed appropriate	15 (75%)	6 (50%)	21
1	Headquarters crisis management plan that describes the crisis management team's and members' responsibilities (headquarters level)	14 (70%)	7 (58%)	21
1	Postincident actions (eg, reporting, analysis) in local security plans	16 (80%)	4 (33%)	20
1	Agency response to employee being taken hostage and to demands for ransom or protection money	14 (70%)	6 (50%)	20
1	Procedure for individual responses to incidents	15 (75%)	3 (25%)	18

*Cited by 16 or more organizations, and cited in 21-30 material sources. Although categorization was done on the basis of all types of documents, scoring as presented includes only staff security manuals and policy/guidelines documents.

† Subcomponent added by research staff for the purposes of this review; not originally included in the InterAction MOSS guidelines.

TABLE 4

Least Commonly Cited Issues in Organizations' Security Policies, Guidance, and Training Materials*

Standard No.	Description of Subcomponent	No. Organizations Citing Item in Security Manuals (of 20)	No. Organizations Citing Item in Security Policies/ Guidelines (of 12)	Total
	Conceptual/analysis-oriented security management subcomponents			
3	Consideration of threats to national staff incorporated into staffing decisions (eg, whether to fill a position with national or expatriate staff)	7 (35%)	5 (42%)	12
3	Security awareness is incorporated into all job descriptions	5 (25%)	5 (42%)	10
3	Make efforts to anticipate emerging security threats that could warrant additional security duties (amend job descriptions as necessary)	5 (25%)	5 (42%)	10
3	National staff trainers and national staff security issues are included in security training curriculum	5 (25%)	4 (33%)	9
3	Orientation materials for national staff include history, role, mandate, and message of the organization	4 (20%)	4 (33%)	8
	Practical security management subcomponents			
3	General explanation of coverage to staff and greater detail when requested on life, workers' compensation for work-related injuries, and health insurance	6 (30%)	5 (42%)	11
4	Staff evaluations include review of security-related responsibilities, if any	4 (20%)	4 (33%)	8
3	General explanation of coverage to staff and greater detail when requested on war risk supplemental coverage in countries excluded from standard insurance plans	2 (10%)	5 (16%)	4

*Cited by 5 or fewer organizations and cited in 1-10 material sources.

and telecommunications, whereas others such as risk assessment frameworks and security management approaches are more conceptual. In practice, this division may be arbitrary and many of the practical subcomponents are based on larger conceptual issues. The distinction was made primarily to facilitate the review of listed subcomponents.

Key Security Management Issues: Similarities and Differences Across Organizations

The most commonly cited messages tend to be found in a greater proportion of security manuals compared to policy documents, whereas the opposite is true for the least commonly cited messages. Although there is often variation across organizations in the level of detail apportioned to specific topics, the content of several most commonly cited messages is similar across organizations, especially those related to procedures. For example, guidance on the use of armed security, although hotly debated within humanitarian circles, is uniformly presented by organizations as a measure to be avoided. The content of several most commonly cited security messages that are more conceptual varies across organizations. Further review illustrates points of commonality and divergence across organizations in the following most commonly cited, conceptually based subcomponents: threat/risk assessment processes; frameworks for determining unacceptable risk; and guidance on acceptance, protection, and deterrence approaches.

Threat/Risk Assessment Processes

THREAT, RISK, AND VULNERABILITY. The majority of organizations cite the importance of conducting a security assessment by describing it as the basis of any security plan and the means by which to identify appropriate measures to mitigate risks.

Eighteen organizations incorporate security assessment guidelines into their manuals. Eight of the 12 policy documents also reference security assessment. The guidelines, in general, contain a similar framework, with comparable concepts and definitions; however, they range in level of guidance from a few sentences or paragraphs covering definitions, concepts, and formulas, to several pages focusing on the purpose of each assessment, including guidelines, checklists, matrices, graphs, and worksheets. Of the 18 security manuals that cover security assessments, 3 provide relatively low detail, 7 provide well-developed detail, and the rest fall between these boundaries.

Across organizations, the stand-alone sections are generally structured around the same conceptual framework (risk = threat × vulnerability) and address each component of the risk formula in a subanalysis. Security assessment guidance typically includes understanding and identifying threats (threat analysis), determining the degree of vulnerability to threats (vulnerability analysis), and considering probability and impact (risk assessment). Often, organizations identify the assessment of political context as a precursor to the security assessment. Few organizations indicate that security assessments

are not a 1-time event or provide guidelines to determine when security assessments should be repeated. Even fewer organizations provide guidance about who should be involved in the security assessment process.

THREAT ASSESSMENT. Across organizations, the definition of a threat is fairly uniform, based on any danger to an organization, its staff, and or its property. The purpose of a threat assessment is also similar across organizations. However, the level of detail in the framework, guidance, and tools ranges significantly. Nearly all organizations state the importance of determining the type and nature of the threat. Indirect and direct threats are the 2 types of threat that are most commonly listed. Crime/banditry is often, but not always, listed as a third type. Guidance generally consists of questions that help staff to understand the nature of a threat. Most organizations recommend that staff use interviews for gathering needed information. Checklists are the next most commonly cited tool, followed by incident reports. Few organizations provide guidance about whom to interview or mention specifically that national staff should be included in the process.

Organizations typically provide guidance in ranking identified threats. The most commonly cited criterion for prioritizing threats is geography followed by frequency and impact. Vulnerability was the least commonly cited criterion. The most common tools for ranking threats by geography, frequency, and impact is mapping of incidents and pattern/trend analysis. Few organizations mention the importance of identifying possible future threats.

VULNERABILITY ASSESSMENT. The definition of vulnerability assessment as a process that determines the degree of susceptibility and exposure to the identified threats is uniform across organizations. There are similarities between organizations in the structure of the vulnerability assessment process, although the degree of guidance varies. Most organizations base their analysis on the understanding that not all organizations, nor all of the staff within the same organization, possess the same degree of vulnerability to the same threat. Nearly all organizations state that it depends on a number of factors, most commonly identified as location (10) followed by image of staff and program (8) and the adoption of, or lack of, appropriate security measures (7). Commonly listed were sex (6), job activities/ responsibilities (6), nationality (6), ethnicity (6), impact of programs (5), staff compliance with security measures (4), and staff interpersonal skills (4). The least commonly listed factors were mission and objectives (3), value of property (3), experienced vs inexperienced staff (3), identity (3), communications (3), affiliations (3), exposure to threats (2), community relations (1), and cultural sensitivity (1).

Framework for Determining Acceptable and Unacceptable Risks

NGOs typically provide guidance for determining when risks have reached an "unacceptable level," described as the point at which available security measures can no longer sufficiently reduce the likelihood of an incident, such that the level of exposure to the threat cannot justify continued operations. In only a few cases is the security assessment process linked to determination of unacceptable risk.

The review found considerable variation in organizations' terminology related to the determination of unacceptable security risk. Although the majority of organizations refer to acceptable vs unacceptable risk, others focus on specified threshold levels. Only 2 of the 20 organizations reviewed specifically mention the term "unacceptable risk"; however 14 organizations, although not specifically referencing this, provide a framework to determine acceptable vs unacceptable risk to an organization's employees, assets, and image. Within the security materials of these 14 organizations, guidance is provided either through a risk matrix and the mapping of a threshold of acceptable risk or through risk or security levels.

THRESHOLD OF ACCEPTABLE RISK. Seven of the 14 organizations reference a threshold of acceptable risk defined as "the point beyond which you consider the risk too high to continue operating so that you must withdraw yourself from that danger zone."[12] All 7 define the threshold in a similar fashion and describe it as the last step in the assessment process. It involves graphing identified risks, with probability of the event on the x-axis and potential impact on the y-axis. Each axis uses the same scale of extremely low to high or catastrophic as a measure of intensity. Although the threshold line connecting impact and probability may differ across organizations, all that reference this concept are in general agreement that the threshold is reached when security measures are unable to sufficiently mitigate the risk or the likelihood of an event to permit the continuation of work.

Variation in determining a threshold of acceptable risk is expected due to varying NGO missions, scopes of work, and mandates. Most organizations indicate that the threshold also depends on the activities being implemented. One organization identifies proportional risk as the basis for its decisions about continuing operations in risky environments, whereby an organization does not work where the risks to staff are more threatening to life than the needs of the population they are serving. All organizations, although not using the term *proportional risk*, are in general agreement that the benefits of the organization's activities should always outweigh the level of risk to staff.

SECURITY/RISK LEVELS. Two of the 14 organizations that provide a framework for unacceptable risk reference a security threshold rather than a threshold of acceptable risk. The security threshold is determined by specific security-related events rather than a measure of probability and impact of threats. The security threshold is most often defined as a readily identifiable trigger event that changes an organization s security measures. For the 2 organizations

that use this term, the highest risk rating (severe risk) describes the point at which the organization considers the level of risk too great to continue its operation (aid workers are directly threatened and humanitarian operations are hindered). The other 12 organizations also provide security or risk levels in which the highest security/risk level calls for project suspension and/or evacuation of staff, although the terminology for the levels differs across organizations as does the identification of indicators for determining the highest risk level. Within the highest security/risk level of all of the organizations, the most commonly listed indicators are the targeting of humanitarian workers (11), the targeting of the organization (8), and the inability to carry out programs (7). Commonly listed indicators include civil unrest (5), collapse of public services (5), indiscriminate violence (5), and open war (4). The least commonly listed include unacceptable risk (2), direct targeting of staff (2), economic collapse (2), collapse of law enforcement mechanisms (2), large-scale mobilization (2), and closure of airports (2).

Guidance on Acceptance, Protection, and Deterrence Approaches

Sixteen organizations reference the 3 security approaches of acceptance, protection, and deterrence, also known as the "security triangle," originally identified by Van Brabant.[12] Ten organizations refer to them as security strategies, and 4 refer to the same concepts as security approaches. One includes acceptance only within its personal security guidance and another mentions all 3 in a country-specific security plan but not in the organization s global security documents. The level of detail provided about security management approaches varies. In some manuals descriptions are limited to a few sentences, while others include an entire section on the conceptual orientation of each strategy, identification of threats each is designed to address, recommended activities, and the advantages and disadvantages of each approach. Of the 16 security manuals that include these concepts, 2 offer a low level of detail, 6 provide relatively well-developed detail, and 8 fall in between the 2 parameters.

Across organizations, the definition of acceptance, deterrence, and protection is fairly uniform. For most, acceptance is described in terms of close/good relationships with the community, ensuring that the community and local authorities understand what they are doing and how beneficiaries are selected, listening to local people, and building good communications with communities, which creates networks, partnership, impartiality, and transparency. Such aspects of acceptance are linked to basic program management.[13] Six organizations emphasize the importance of engaging with local authorities, whereas most focus on the community at large. The emphasis on meetings and stated messages and the politics of staff composition, as included in the Van Brabant acceptance framework, are mentioned consistently by 1 organization and less consistently by 3 others. Half of the NGOs that discuss acceptance articulate the notion that NGOs cannot take for granted that communities know, understand, and accept what they are doing. These organizations explicitly identify acceptance as something that must be built up, won, and maintained, often referred to as active acceptance.

Six organizations explicitly state that acceptance is their preferred strategy. Others do not indicate a formal preference but direct staff to use a mix of approaches to create a balanced strategy depending on the operating environment. Half of the organizations indicate that deterrence is not a preferred approach, using phrases such as "not advocated," "ordinarily not the preferred method," "needs to be considered carefully," "last resort," and to be used "under exceptional circumstances." For most organizations, deterrence strategies translate into threat of withdrawal in retaliation for a seriously deteriorated security situation and the use of armed guards. A few organizations direct staff to seek guidance or approval from senior management at the headquarters level before pursuing a deterrence strategy.

DISCUSSION

Few of the 20 organizations cover all or even most of the InterAction MOSS subcomponents, and some are more frequently included than others. The InterAction MOSS content is heavily oriented toward standard 1 (organizational security policy and plan) and many subcomponents are activities that NGOs were most likely implementing before its development. Therefore, it is not surprising that standard 1 subcomponents are well covered by most organizations.

Subcomponents under standard 3 (human resource management) are not frequently mentioned in security documents, although some of the least commonly cited issues may be addressed by human resources departments. There is value in underscoring linkages between security and human resources in the mindset of both the organization and its staff. Staff need clarity about insurance availability within the context of local security conditions, and organizations must regularly assess program coverage in high-risk situations. This may already happen in some organizations, but formalizing the connection through written security guidance can help ensure that these processes take hold. Formally requiring, within security guidance, that security awareness be incorporated into all job descriptions and that performance evaluations include security-related responsibilities helps ensure that staff responsibilities are actualized.

National staff security is an issue of obvious importance. Rowley et al found that of all intentional violence events across 18 international humanitarian organizations between September 2002 and December 2005, 58% occurred to national staff.[2] Stoddard and colleagues have reported that from 1997 to 2005, 79% of all aid workers who were killed, kidnapped, or wounded due to security-related reasons as

reported in their incident tracking system, were national staff.[3] The proportion of national staff affected was 89% in 2006, 83% in 2007, and 81% in 2008.[5] Several of the least commonly cited subcomponents relate to human resources management and national staff. It is possible that these activities occur in the field without being formally included in the security policy and guidance of organizations. Of all of the security issues specifically addressing national staff, the most common guidance relates to local security plans and the extent to which the organization is committed to the evacuation or relocation of national staff in an emergency. This focuses attention on the level of liability that an organization is willing to accept for national staff in a deteriorating security situation, rather than acknowledging that program plans must incorporate from the outset any risks that national staff may face.

For several years, national staff security training has been a concern.[2,3,7,14,15] Stoddard et al have noted that even in highly dangerous environments, many NGOs focus security training on international staff[3]; they more recently reported that humanitarian organizations may be extending security training to national staff in part in an effort to ensure increased equity, although national staff may face different risks than expatriates in some settings.[5] The inclusion of national staff trainers and national staff security issues in training is 1 of the least commonly cited subcomponents in the available guidance documents of the 20 organizations reviewed. There continues to be a mismatch between organizations' lack of emphasis on understanding and formally incorporating national staff security issues into security management, and the risks that they encounter. Given that most NGO staff are nationals, it is of great concern that they do not receive comprehensive security training and that their experiences, perspectives, and concerns are not always formally emphasized in security documents.

Security management involves personnel, equipment, training, and other costs that have taken many organizations years of internal lobbying and donor advocacy to develop, yet funding for security remains low. The International Medical Corps reports that among 21 headquarters-based staff surveyed, 70% indicated that their organization's security budget ranged from 0.05% to 1% of annual revenue.[16] The streamlining of security costs into program budgets and strategic planning for the financial implications of security management (standard 2) is rarely mentioned in the security documents reviewed, although directives on security costs may be found in other program development guidance documents. The focus on security resource needs is well placed within the MOSS and NGOs should incorporate this guidance in security documents. Accountability for security (standard 4) is inherently controversial. Although public lawsuits against humanitarian organizations are rare, out-of-court settlements may not be, and NGOs are keenly aware of their responsibilities to protect staff. At the same time, the emphasis on staff members' own responsibilities for security was 1 of the most frequently mentioned subcomponents, reflecting the importance of reminding staff of their role in security management and the organizations' need to minimize legal responsibility for rapidly changing security conditions and individual staff behavior.

Although there has long been a call for coordinated security event information, this has been both problematic and slow in coming.[4] Reasons include lack of resources and reluctance to openly disseminate details about security events that could increase liability. This review demonstrates that at a policy and guidance level, staff are encouraged to share security information, yet the practicalities of doing so remain undefined and left to the discretion of people in the field. It will not be a consistent practice unless systems and procedures for the collection of comparable information and information sharing are developed.

There are 2 key findings in determining the types of documentation NGOs most often use to communicate key security messages. First, although all 20 organizations have some form of security manual, only 12 have specific security policy documents. Stated security policies provide an important reference point for aid workers and those with whom they interact, including host governments, donors, local leadership, and community members. Issues that are covered typically in security policies, such as prohibition of staff use of weapons, are crucial for staff to understand and be able to communicate. A written policy document would clarify key security concerns to staff, help them realize their responsibilities, and support their interactions with others.

Second, the dearth of readily available training materials is not an indicator of inadequate staff security training per se, but rather a symptom of scattered, ad hoc approaches to security training within many organizations. Aid workers' views on security training are mixed at best. A little more than half (55%) of 1294 aid workers in a 2005 survey by Buchanan and Muggah indicated that the security training they received had been either very helpful or helpful.[14] An assessment of humanitarian staff security perceptions in 2007 by Fast and Wiest found no significant differences in perceptions about insecurity among those who received training and those who did not.[15] More recently, Stoddard and colleagues, in their research on private security providers, reported that some interviewees believe training programs do not reflect changing security realities on the ground and focus more on security awareness and basic concepts than on practical security guidance.[17] InterAction's ongoing efforts to create a professional association for the humanitarian security sector aim in part to address training standards; however, a systematic review of security training content and an evaluation of security training effectiveness remain necessary.[2-4,7]

Review results provide important insights on divergences across organizations on 3 of the most commonly cited security

guidance points. First, although the general terminology and frameworks used to describe security risks and security assessment are comparable across organizations, the level of guidance offered on the implementation of assessments varies. Notwithstanding previous security assessment experience, this divergence implies that staff at different organizations in the same location will have varied levels of guidance and training in how to understand the security environment. NGO staff should have access to a minimum level of guidance about how to conduct a security assessment and how to link assessment results to an interpretation of risk.

Organizations working in the same location often make different security-related decisions based on their perceptions about risk and vulnerability. This is to be expected because security vulnerability depends on a range of factors that are specific to individual organizations including mission and organizational identity, staff size, and program value and activities. Organizations will uniquely interpret their positions on a risk curve or in relation to risk levels, depending on their own definition of vulnerability, but differences in the definitions, processes, and tools in determining risk may complicate communication and collaboration across organizations.

Lastly, most organizations link the assessment process to the determination of which security approaches to use. Although acceptance is often described as the preferred approach, there may be room for different types of acceptance efforts depending on the intensity of risk. This is not something that has been formally explored. Rather, increased intensity of security risks typically engenders more protection and deterrence-oriented strategies. Some within the humanitarian community question whether organizations have become overly reliant on acceptance in light of worsening security in many settings.[3,18] the present review indicates that many organizations understand and articulate only part of the original acceptance concept. Many of Van Brabant s details on issues such as interactional and negotiating styles, the nuances of appropriate socializing and diplomacy, messages and images conveyed through meetings, and real or perceived divisions among staff are not emphasized.[12] In addition, many organizations do not distinguish between passive acceptance, with the assumption that undertaking programs in a community automatically translates into acceptance, and active acceptance, which must be established and maintained consistently. Further consideration of what acceptance means, how it is implemented, and the impact it can be expected to produce on the security of both national and expatriate staff is timely in light of ongoing revisions to the security management framework.

Limitations

A number of limitations relate to this research. First, cutoffs other than those used for the categorization of most and least commonly cited security issues could create a somewhat different constellation of key messages, although it is likely that the overall picture generated would be similar. Second, the present review has focused on the subcomponents that were found to be most and least commonly cited. A closer review of subcomponents in the middle would likely yield some additional observations. Third, we were limited in the number of issues selected for further analysis and focused on subcomponents, where we saw immediate differences. A more comprehensive analysis of similarities and differences across a greater number of subcomponents could be instructive.

The review was not able to collect many organizations' training documents. Only 5 organizations provided training materials for review and these were limited to generic, agency wide training materials. In addition, organizations may cover certain subcomponent topics, such as those related to human resources management and budgeting for security, in policies and guidance generated by departments outside security. The efforts of NGOs to cross-reference other policy documents and state the security aspects of other departments' activities and policies would be well placed.

InterAction members are required to be "MOSS compliant." European, Japanese, and other NGOs may also use the InterAction MOSS, but likely consider a number of other resources and criteria when designing their security materials. Major differences between US-based organizations and others were not noted, however.

CONCLUSIONS

The InterAction MOSS is a crucial contribution to humanitarian security management, yet gaps exist in NGO manuals and policies that can hinder efforts to garner needed resources, clarify security responsibilities, and ensure that the distinct needs of national staff are recognized and addressed. A common terminology and conceptualization of analytical processes in security management, such as security assessment, risk determination, and security management approaches, would strengthen the efforts of organizations to collaborate on security without compromising autonomous decision making.

The humanitarian community should also consider an evidence-based view of what works in security management. A further step toward determining effectiveness is to investigate how these messages are interpreted by staff. This can be done through a field-based review of security practices in relation to existing policies and other security-related communications.

The humanitarian community has made great progress in the development of practical staff security guidance during the past 10 years, but this is an evolving process that must adapt to ever-changing security realities. As this review demonstrates, further investments in the refinement of security guidance and training are warranted.

About the Authors

The authors are with the Center for Refugee and Disaster Response, Johns Hopkins Bloomberg School of Public Health.

Address correspondence and reprint requests to Elizabeth Rowley, Center for Refugee and Disaster Response, Johns Hopkins Bloomberg School of Public Health (e-mail: erowley@jhsph.edu).

Acknowledgments

The authors gratefully acknowledge the Bureau of International Cooperation of the International Medical Center of Japan for the financial support of this research. We also thank the following individuals for reviewing earlier drafts of this article and providing helpful comments on its content: Mari Nagai, Frederick Burkle, John Schafer, Michael O'Neill, Larissa Fast, and Madeleine Kingston.

Received for publication November 20, 2009; Accepted May 25, 2010.

REFERENCES

1. Sheik M, Gutierrez MI, Bolton P, Spiegel P, Thieren M, Burnham G. Deaths among humanitarian workers. *BMJ*. 2000;321(7254):166-168.
2. Rowley EA, Crape BL, Burnham GM. Violence-related mortality and morbidity of humanitarian workers. *Am J Disaster Med*. 2008;3(1):39-45.
3. Stoddard A, Harmer A, Haver K. *Providing Aid in Insecure Environments: Trends in Policy and Operations*. Humanitarian Policy Group Report 23. London: Overseas Development Group; 2006.
4. Bollettino V. Understanding the security management practices of humanitarian organizations. *Disasters*. 2008;32(2):263-279.
5. Stoddard A, Harmer A, DiDomenico V. *Providing Aid in Insecure Environments: 2009 Update*. Humanitarian Policy Group Policy Brief 34. London: Overseas Development Group; 2009.
6. Van Brabant K. Security training: where are we now? *Forced Migration Rev*. 1999;4:7-10.
7. European Commission Humanitarian Aid Office. *Report on Security of Humanitarian Personnel: Standards and Practices for the Security of Humanitarian Personnel and Advocacy for Humanitarian Space*. Brussels: ECHO; 2004:3.
8. Van Brabant K. Cool ground for aid providers: towards better security management in aid agencies. *Disasters*. 1998;22(2):109-125.
9. InterAction. Minimum Operating Security Standards. May 2006. *http://www.eisf.eu/resources/library/IA_MOSS_1.pdf*. Accessed June 15, 2010.
10. InterAction. Suggested Guidance for Implementing InterAction's Minimum Operating Security Standards. June 2006. *http://www.interaction.org/sites/default/files/MOSS_Implementation_May_2006.pdf*. Accessed June 15, 2010.
11. InterAction. *The Security of National Staff: Essential Steps 2002*. Washington, D.C.: Interaction; 2002.
12. Van Brabant K. *Operational Security Management in Violent Environments: A Field Manual for Aid Agencies*. Good Practice Review 8. London: Humanitarian Practice Network/Overseas Development Institute; 2000:58.
13. O'Neill M. Acceptance: an approach to security as if people mattered. *Monday Dev*. January/February 2008;26:22-24.
14. Buchanan C, Muggah R. No Relief: Surveying the Effects of Gun Violence on Humanitarian and Development Personnel. Geneva: The Centre for Humanitarian Dialogue and The Small Arms Survey; 2005.
15. Fast L, Wiest D. *Security Perceptions Survey Final Report*. South Bend, IN: University of Notre Dame, Kroc Institute for International Peace Studies; 2007.
16. International Medical Corps. *Security Management in Humanitarian Agencies*. Santa Monica, CA: International Medical Corps; 2009.
17. Stoddard A, Harmer A, DiDomenico V. *The Use of Private Security Providers and Services in Humanitarian Operations*. Humanitarian Policy Group Report 27. London: Overseas Development Institute; 2009.
18. Macpherson B, Persaud C, Sheehan N. Experienced advice crucial in response to kidnappings. *Monday Dev*. March 2008;26:22-24.